



## **Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks**

**Meng, Weizhi; Choo, Kim-Kwang Raymond; Furnell, Steven; Vasilakos, Athanasios V.; Probst, Christian W.**

*Published in:*  
IEEE Transactions on Network and Service Management

*Link to article, DOI:*  
[10.1109/TNSM.2018.2815280](https://doi.org/10.1109/TNSM.2018.2815280)

*Publication date:*  
2018

*Document Version*  
Peer reviewed version

[Link back to DTU Orbit](#)

*Citation (APA):*  
Meng, W., Choo, K-K. R., Furnell, S., Vasilakos, A. V., & Probst, C. W. (2018). Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks. *IEEE Transactions on Network and Service Management*, 15(2), 761-773. <https://doi.org/10.1109/TNSM.2018.2815280>

---

### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks

Weizhi Meng, *Member, IEEE*, Kim-Kwang Raymond Choo, *Senior Member, IEEE*, Steven Furnell, Athanasios V. Vasilakos, and Christian W. Probst

**Abstract**—The medical industry is increasingly digitalized and Internet-connected (e.g., Internet of Medical Things), and when deployed in an Internet of Medical Things environment, software-defined networks (SDN) allow the decoupling of network control from the data plane. There is no debate among security experts that the security of Internet-enabled medical devices is crucial, and an ongoing threat vector is insider attacks. In this paper, we focus on the identification of insider attacks in healthcare SDNs. Specifically, we survey stakeholders from 12 healthcare organizations (i.e., two hospitals and two clinics in Hong Kong, two hospitals and two clinics in Singapore, and two hospitals and two clinics in China). Based on the survey findings, we develop a trust-based approach based on Bayesian inference to figure out malicious devices in a healthcare environment. Experimental results in either a simulated and a real-world network environment demonstrate the feasibility and effectiveness of our proposed approach regarding the detection of malicious healthcare devices, i.e., our approach could decrease the trust values of malicious devices faster than similar approaches.

**Index Terms**—Intrusion Detection, Software-Defined Networking, Trust Computation and Management, Healthcare Network, Bayesian Inference.

## I. INTRODUCTION

WITH rapid developments in information and communications technologies (ICT), healthcare organizations are moving towards employing many of the same infrastructure elements, applications, off-the-shelf technologies, and processes used by organizations in other sectors. This is not surprisingly, as networked or Internet-connected medical devices can facilitate more effective management of assets, electronic health records, communications, etc, which results in reduced costs (e.g., associated with monitoring and treatments). A report estimated that networked technologies may

save much money for healthcare organizations for the next few years, i.e., it can reduce the costs for hospital equipment by a 15-30 percent [11].

While security of devices and systems, and privacy of user data, are two key considerations in most information systems, security and privacy are particularly important factors in a healthcare setting due to the exacting requirements of the industry (e.g., the Health Insurance Portability and Accountability Act of 1996 for U.S.-based healthcare organizations). Hence, it is of little surprise that a recent McAfee report identifies that networked medical devices may expose security gaps when the medical industry tried to combine all technology aspects regarding operational controls and networked infrastructure [17]. In addition to the sensitive nature of the data in healthcare networks, the complexity, number and diversity of devices, especially networked medical devices (e.g. wireless pacemakers), that make up this infrastructure expose such networks to a broader range of security and privacy risks [4], [12], [41], [47]. For instance, the number of information security breaches reported by healthcare providers has an increase by 60 percent in 2014, which is nearly double the rate found in other domains [15]. As evidenced by the recent ransomware incidents [5], [20], it is clear that the healthcare industry is not immune to cyber attacks. The latter could be due to accidental failures, privacy violations (e.g., leakage or compromise of sensitive medical records), intentional and/or widespread disruption (e.g., due to vulnerabilities and/or flaws in design, implementation and operation).

In recent times, researchers have started exploring the potential of deploying software-defined networking (SDN) in healthcare organizations, since SDN can abstract network policy from network devices, eliminate device level configuration and provide an open networking model for consolidation [33]. In the context of cyber security in healthcare organizations, SDN can be used to defend a medical network against a range of attacks (e.g., denial-of-service and flooding attacks). However, similar to existing or conventional security solutions such as intrusion detection and prevention systems or centralized protection approaches, SDN solutions do not generally protect the system and data from insider attacks [16], [32], [38]. For example, 92% healthcare organizations expressed concerns that their organizations suffered from insider threats and required suitable protection solutions [43]. This necessitates the design of effective solutions to mitigate insider threats.

In this work, we target on the detection of insider malicious

W. Meng is with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark.  
E-mail: weme@dtu.dk

K.K.R. Choo is with the Department of Information Systems and Cyber Security and the Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, United States.  
E-mail: raymond.choo@fulbrightmail.org

S. Furnell is with the School of Computing, Electronics and Mathematics, Plymouth University, United Kingdom.  
E-mail: S.Furnell@plymouth.ac.uk

A.V. Vasilakos is with the Department of Computer Science, Lulea University of Technology, Sweden.  
E-mail: athanasios.vasilakos@ltu.se

C.W. Probst is with the Unitec Institute of Technology, New Zealand.  
E-mail: cprobst@unitec.ac.nz

devices in a healthcare SDN. More specially, we survey stakeholders from 12 healthcare organizations (four located in Hong Kong, four located in Singapore, and four located in China) to have a better understanding of the real-world requirements. Informed by the findings of the survey, we describe the typical architecture of healthcare SDNs and develop a detection approach by using Bayesian model to figure out malicious devices inside such network. Specifically, in our approach, after identifying malicious devices, the SDN controller can easily update flow tables and guide traffic to bypass those malicious points. To the best of our knowledge, this is one of the earlier work in this area (i.e., identification of malicious devices for healthcare SDNs). We then evaluate the proposed approach in either a simulated and a real network environments (two of the 12 surveyed organizations located in China) under different scenarios.

We would also clarify that this paper focuses only on the identification of insider attacks using trust computation, rather than how we can improve an intrusion detection system (IDS). However, our proposed approach can be used to complement existing security solutions. While we use the healthcare organization as an application domain, the proposed approach can be applied to a generic SDN-based network.

In Section II, we introduce SDN and related work regarding trust management in WSNs and distributed IDS networks. Section III reports on the usage of Internet-enabled devices in the healthcare sector and introduces the reference SDN architecture used in this work. In Sections IV and V, we present our proposed trust-based approach and its evaluation. Section VI discusses limitations and open challenges in this field. Finally, Section VII concludes our work.

## II. BACKGROUND AND RELATED WORK

In this section, we introduce the background of software-defined networking and present relevant studies regarding trust management in various network environments.

### A. Background on SDN

A typical SDN is composed of many programmable switches and control entities, with the purpose of migrating networking functionality into a user-definable interface. SDN is an emerging architecture that provides many demanding features like dynamics, management, cost-effectiveness and adaption. Unlike traditional networks, SDN can deploy additional components to its architecture, i.e., adding any software that can work inside a server or a CPU. This allows the migration of network functionality to a defined software interface. In other words, the network's control plane is a kind of software component [24].

Fig. 1 depicts the three-layer SDN architecture. The first layer is the application layer, which is responsible for enforcing policies via the northbound APIs supported by the control layer (the second layer). In comparison, southbound APIs are used to support the interactions between the control and the third layer - the infrastructure layer. The SDN controllers can perform as a strategic control point in the network to manage flows for switches, applications and policy engines. In

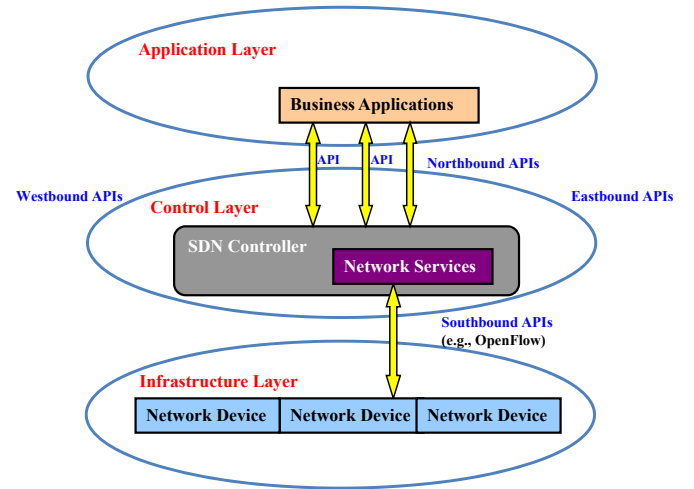


Fig. 1. A three-layer SDN architecture, comprising the application layer, the control layer and the infrastructure layer.

such a centralized architecture of network management, users do not need to notice network topology and the underlying physical network, which can significantly reduce the workload for designing the whole network including various operations. With a SDN controller, organizations or users are able to obtain independent control of the whole network from a single and logical point.

More specifically, due to the centralized control in SDNs, users can monitor and manage network events at the application layer in real-time, and implement new services (or applications) in a quick manner. These capabilities can help users utilize common network services (e.g., routing and multicast) to achieve their either individual or organizational goals. As an example, users can deploy related APIs between the controller and the applications, and then work on the network abstraction through leveraging network services without the need to be know the specific implementation details. Therefore, when a new flow arrives at a switch in SDNs, this switch is able to know the forwarding path by sending a routing request to the centralized controller. It is worth noting that the controller has to generate a routing path and exchange the forwarding rule, via a secure channel, with all the related switches. After receiving the rule, all corresponding SDN switches can make an update to the flow tables.

On the whole, SDN can easily manage the whole network and offer various benefits like allocating on-demand resources and providing secure cloud services, because of its global view and the centralized control. One specific benefit of the SDN application is to enable network abstraction, which offers an easy way for users to configure a service without the need to understand the network complexity. From the view of devices, they only need to accept instructions from the corresponding SDN controllers and there is no need to know the thousands of protocol standards in practice. Furthermore, SDN can provide more flexibility than the conventional networks. For instance, SDN controller based on software can be easily modified or re-configured for better interaction among different components, as compared with hardware-based devices.

## B. Related Work

The healthcare SDN manages a set of distributed entities, in which this distributed nature is similar to that structure of a wireless sensor network (WSN). In literature, there are only a small number of studies on building trust management in healthcare SDN to defend against insider attacks. For real-world implementation, WSNs and healthcare networks may employ different topologies, while the trusted IDS principles are still the same. Therefore, this section introduces existing approaches on how to establish trust management for WSNs and distributed IDS networks.

**Intrusion detection systems (IDSs).** These systems are usually deployed to identify any behavioral anomalies or policy violations through monitoring the protected networks and systems. Typically, an IDS can be classified into two categories: signature-based IDS and anomaly-based IDS. The former detects attacks by matching network or system events with available signatures [34], [35]. A signature (or rule) is a kind of descriptions of a known attack or exploit, which determines the detection capability in real-world applications (i.e., its detection accuracy would not be better than its available signatures). The latter first builds a profile for typical activities on the target computer and network, and then identifies potential anomalies if the deviation between the monitored events and the normal profile exceeds a pre-defined threshold [10]. Alarms will be generated if anomalies are discovered. To improve the detection performance, distributed and collaborative IDSs are often applied in real-world environments [45], [51].

**Trust management for wireless sensor networks.** The notion of *trust* in computer science derives mainly from the field of social science, aiming to predict and judge the situations of an object [9]. In literature, many trust-based approaches with intrusion detection technology have been developed and studied, [7].

To establish trust management among WSN nodes, Probst and Kasera [36] proposed a distributed and statistical trust, which used a confidence interval to explore the behavior of sensor nodes. It can be utilized to evaluate the reputation among many nodes, identify malicious or malfunctioning ones, and reduce their impact on network performance. Wang *et al.* [37] focused on mobile Ad hoc networks (MANET) and designed a detection approach to look for malicious sensor nodes. Two trust values were developed for node evaluation: Evidence Chain (EC) and Trust Fluctuation (TF). Chen *et al.* [6] introduced a trust management approach based on network events, which employed the watchdog method to monitor nodes events and then broadcast the trust values of nodes. In particular, their approach assumed that each node can own more than one trust values and their neighbor nodes have to store these values for trustworthiness evaluation.

Then Shaikh *et al.* [39] gave a group-based approach of evaluating the trustworthiness of nodes organized in a cluster, which integrated both direct and indirect trust. Their approach considered two network topologies: one is *intragroup topology* which was suitable for distributed trust management; the other one is *intergroup topology* which adopts a centralized

trust management approach. Guo *et al.* [13] presented a trust management framework to generate trust values by means of Grey theory and Fuzzy sets. The final trust value in their work was calculated using relation factors and weights of neighbor nodes, not just by simply taking an average value.

In addition to direct trust, it is also feasible to leverage indirect trust information. Zahariadis *et al.* [49] designed a routing protocol that identify unusual nodes by means of both direct and indirect trust. This distributed trust model could handle different network dimensions via the geographical routing principle. Zhang *et al.* [50] introduced a dynamic trust management method to evaluate trustworthiness for hierarchical WSNs, through combining both direct and indirect trust. They also considered the movement of nodes from clusters and gave a higher weight to the most recent events via a trust varying function. Bao *et al.* [2], [3] designed a detection approach for identifying malicious nodes in hierarchical WSNs by means of quality of service (QoS) trust and social trust. The evaluation demonstrated a better detection accuracy and a lower false positive than conventional IDSs.

**Trust management for distributed IDS networks.** To enhance the detection performance of a single IDS, distributed or collaborative IDS networks have been widely developed through enabling the information collection and exchange among a set of IDS nodes [48].

Li *et al.* [21] figured out that both centralized and distribution fusion could be unscalable for current distributed IDSs due to communication issues. To solve this issue, they constructed a distributed detection system based on decentralized location and routing framework. One weakness of their approach is that they considered all peers were trusted though these peers are vulnerable to insider threats. This assumption makes their system unrealistic in practical scenarios. Targeted on this issue, Duma *et al.* [8] acknowledged that not all nodes are trusted and developed an Overlay IDS, which could detect malicious nodes via P2P-based intrusion detection. This system managed trust values (i.e., correlating alarms) by means of a trust-aware engine and an adaptive approach. In particular, the engine was able to reduce unwanted alerts sent by untrusted or low reputation peers, and the adaptive approach was able to predict peers' trust values based on their past experiences.

However, peers' past experiences should be used in a careful way, since the older trust information was not beneficial for predicting a nodes' trust value. Focused on this issue, Fung *et al.* [18] developed a Host-based IDS framework to detect malicious nodes through a challenge-based trust mechanism, which allows each node to evaluate the trustworthiness of other nodes through sending challenges and matching the received feedback. They also utilized a forgetting parameter to give more weights on the recent events observed from the target nodes. They then developed a Dirichlet-based approach to compute the trust values among a set of nodes based on their mutual evaluation, which is much scalable in practice and is robust against insider attacks (i.e., some benign nodes turn to sending malicious packets suddenly) [19].

Intuitively, each node may have different detection capability within a distributed IDS network, due to their deployed

signatures and detection algorithms. Li *et al.* [22] advocated this observation and developed a notion of *intrusion sensitivity* to model the detection capability of each node. They then applied this notion for improving the challenge-based trust mechanism and achieved better results than the original scheme [23]. They further identified how to allocate the values of intrusion sensitivity remains a challenge, and proposed an allocation method by means of machine learning algorithms, which could greatly reduce human efforts for value assignment [25]. In addition to the challenge-based trust mechanism, trust management of distributed IDS networks can be also built by using information theory [42] and game theory [44]. To further enhance the performance of an IDS, many optimization approaches have been designed in literature, such as alarm reduction [26], alarm verification [30], [31] and many filtration mechanisms (e.g., EFM [29]).

**Discussion.** IDSs have also been applied for SDN applications. For example, Ha *et al.* [14] developed a traffic sampling strategy to reduce the processing capability of an IDS in SDN, which samples traffic flows according to defined sampling rates. AlEroud and Alsmadi [1] proposed a detection approach to identify DoS attack in a SDN environment, using an inference mechanism and a packet aggregation technique to create attack signatures and predict attacks.

As SDN has the potential to improve quality of care and protect patient data in healthcare domain, there is a need for healthcare organizations to maintain trust in medical equipment and system. Insider attacks are one of big threats for healthcare networks [16]. However, there are relatively few studies on how to build trust management in SDN to detect insider attacks. Motivated by these, this work focuses on establishing trust management in a healthcare SDN environment to defend against insider attacks.

### III. HEALTHCARE SDN: SURVEY AND ARCHITECTURE

In this section, we first describe our survey of 12 healthcare organizations regarding their usage of Internet-enabled devices, prior to presenting the architecture of healthcare SDNs.

#### A. Internet-Enabled Devices in Healthcare domain

To reduce cost and improve management, medical devices are increasingly connected to the Internet. In this part, we summarize the findings of a survey conducted with stakeholders from four healthcare organizations in Hong Kong (HK), four healthcare organizations in Singapore (SG), and four healthcare organizations in China (CN). The survey was designed to understand the usage of Internet-enabled medical devices in these organizations, and their requirements. The choice of the organizations was a pragmatic decision, based on the authors' existing contacts and collaborations. Participants were enlisted via telephone and email contacts, and their organizations had a significant usage and investment in IT systems. For privacy reasons, Table I mainly describes the size of these organizations (hospitals and clinics).

From the findings depicted in Fig. 2, it is clear that the number of Internet-enabled devices is significant. Reported usage of these devices are as follows:

TABLE I  
PARTICIPATING HEALTHCARE ORGANIZATIONS.

Hospitals	Personnel	Clinics	Number of Personnel
HK Hospital 1	> 300	HK Clinic 1	30-50
HK Hospital 2	200-300	HK Clinic 2	10-30
SG Hospital 1	> 300	SG Clinic 1	40-60
SG Hospital 2	100-200	SG Clinic 2	30-50
CN Hospital 1	200-300	CN Clinic 1	30-50
CN Hospital 2	100-150	CN Clinic 2	10-20

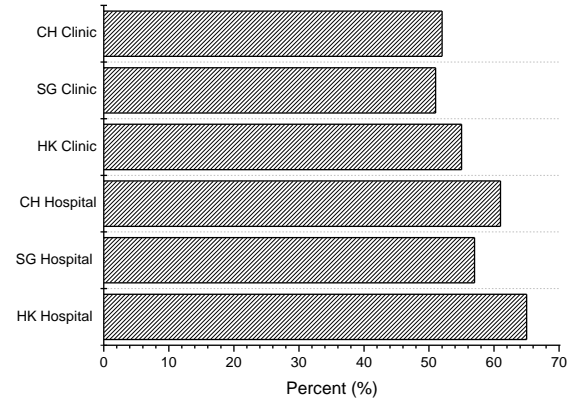


Fig. 2. Reported usage of Internet-enabled devices in the participating healthcare organizations.

- To facilitate record and data management for patients (e.g., storing of patient healthcare records).
- To communicate with other healthcare personnel (e.g., sharing information about surgery time).
- To exchange patient information (e.g., between different departments for handover in patient care).

During the survey, we also sought to understand the system requirements. The key observations are described as below, which are in line with our previous study [32].

- In medical networks, it has to be ensured that all networked devices can operate smoothly. Thus, the adopted security solutions should be able to detect malicious devices dynamically and reduce false positive rate.
- The adopted security solution should provide full-time inspection and management, i.e., monitoring network and device traffic, enforcing security policies.
- Since most healthcare personnel are not information technology (IT) experts, it is important to adopt centralized control (e.g., centralized-decision architecture) in order to identify and respond to intrusions (e.g., betrayal attacks). As a result, a hierarchical structure can help handle intrusions more efficiently.

Furthermore, more than half of these participants reported that SDN technology could be applied in their organizations and emphasized that security is a significant consideration in medical networks.

#### B. Healthcare SDN Architecture

A critical aspect of healthcare partnership is the capability to consolidate systems while maintaining seamless commu-

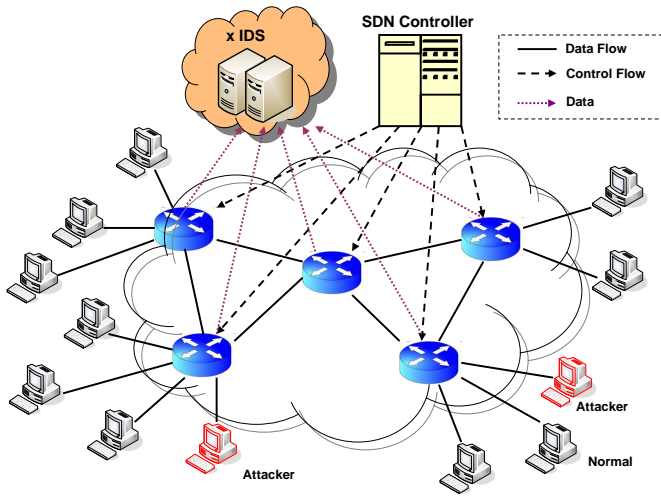


Fig. 3. A typical architecture of healthcare SDNs. ( $x$  IDS means there may be multiple IDSs)

nication throughout the organization. Traditional networks are generally difficult to consolidate, as each network device can contain hundreds of configurations that need to be changed [33]. Thus, SDN is a viable solution, which provides the ability to abstract network policy from network devices, eliminating device level configuration and providing an open networking model for consolidation.

As an example, SDN could be used to provide patient data security as well as the agility required to move the data from endpoint to endpoint [33]. The SDN controller detects when a patient monitoring endpoint connects to the network. Forwarding entries are loaded into the network switches that allow the endpoint to connect only with the patient monitoring controller. The monitoring endpoint can be connected anywhere in the SDN switch network, since the SDN controller will automatically identify the endpoint and connect the ingress interface to the corresponding virtual network, providing reliability, mobility, and security.

Fig. 3 depicts a typical architecture of healthcare SDNs, based on the findings from our survey. Such an architecture composes of an SDN controller, a set of OpenFlow switches and a number of medical devices and client devices (e.g., mobile devices and personal computers). An OpenFlow switch separates the data and control functions of networking devices. The OpenFlow specification provides a standardized way of implementing an SDN architecture, and the OpenFlow protocol can control network switches where to send packets. All these make the whole network programmed independently of the individual switches and data center. Therefore, the SDN controller can collect flow status from each switch and manage its flows easily. For instance, the controller can configure all data packets sent by the OpenFlow switches.

#### IV. OUR PROPOSED APPROACH FOR HEALTHCARE SDN

In this section, we describe how to apply intrusion detection in a healthcare SDN, and introduce the way of calculating devices' trust values and identifying untruthful devices by mean of a Bayesian inference approach.

TABLE II  
KEY TERMS FOR BAYESIAN INFERENCE MODEL.

Terms	Meaning
$P(n_i : normal) = p$	The probability of the $i^{th}$ packet is normal
$V_i$	The $i^{th}$ packet is normal
$n(N)$	The number of normal packets

#### A. Healthcare SDN with IDS deployment

As previously discussed, IDSs are a common security solution for detecting various network and system anomalies. In particular, Snort [40] is a lightweight open-source NIDS with the capability of analyzing traffic in real-time, interpreting protocol and performing signature matching. As shown in Fig. 3, an IDS can be deployed in a centralized server within the healthcare SDN for examining data packets. There are two common deployment approaches available:

- *Single IDS.* This deployment uses only one IDS to control and handle all traffic in healthcare networks, but requires the deployed IDS to have a strong processing and communication capability.
- *Multiple IDSs.* This deployment can use one main IDS and a set of IDS agents. In particular, IDS agents are responsible for handling traffic in SDN/OpenFlow switches (e.g., inspection and statistic recording), whilst the main IDS acts as a controller for data aggregation and communication with the SDN controller.

All these deployment approaches allow switches to send mirrored packets to IDSs. During our survey, it was found that the second option of multiple IDSs was preferred by most participants. This is, perhaps, unsurprising as the second option is more suitable for a distributed network environment. Moreover, in our data-intensive society, traffic volumes will also significant increase. Thus, we focus on the healthcare SDN with multiple IDSs in the evaluation.

#### B. Bayesian Inference-based Trust Management

Bayes' rule is used by Bayesian inference to adjust the probability for a hypothesis as more evidence turns to be available [42]. For trust management, it can be helpful for computing the trustworthiness among network nodes and deciding malicious ones based on defined rules. This approach mainly assumed that all packets delivered by a device are independent from each other. In other words, this assumption indicates that the probability of a packet being malicious is  $1/2$ . This is a reasonable assumption, as practical attackers can send malicious packets in many ways (i.e., with either one or multiple malicious packets). Some key terms relating to the use of Bayesian inference model are described in Table II.

In terms of the results in previous work [9], [42], it is reasonable to assume the distribution of observing  $n(N) = k$  is governed by a Binomial distribution. This distribution shows  $n$  successes out of  $N$  Bernoulli trials, in which each  $n$  has the same possibility  $p$  when the trial is true. Subsequently, if we observe  $N$  packets are delivered by a device, in which  $k$  of them are *benign*, then we can compute the probability of such situation as below.



$$P(n(N) = k|p) = \binom{N}{k} p^k (1-p)^{N-k} \quad (1)$$

The ultimate goal of applying Bayesian inference in this work is to judge whether the  $N + 1$  packet is benign or not (denote  $P(V_{N+1} = 1|n(N) = k)$ ). This probability obeys the distribution based on Bayesian theorem as below.

$$P(V_{N+1} = 1|n(N) = k) = \frac{P(V_{N+1} = 1, n(N) = k)}{P(n(N) = k)} \quad (2)$$

Then we can apply the marginal distribution to the above equation. That is, if  $X$  and  $Y$  are discrete random variables and  $f(x, y)$  is the value of their joint probability distribution at  $(x, y)$ , then the marginal distributions of  $X$  and  $Y$  can be given as:  $\sum_y f(x, y)$  and  $\sum_x f(x, y)$ , respectively. In this case, we have the following Equations 3 and 4:

$$P(n(N) = k) = \int_0^1 P(n(N) = k|p) f(p) \cdot dp \quad (3)$$

$$P(V_{N+1} = 1, n(N) = k) = \int_0^1 P(n(N) = k|p) f(p) p \cdot dp \quad (4)$$

Since we do not have any prior information about  $p$ , it is reasonable to assume that this information is governed by a uniform prior distribution  $f(p) = 1$ , where  $p \in [0, 1]$ . As a result, we can derive the following Equation 5 by considering Equations 1 to 4.

$$\begin{aligned} P(V_{N+1} = 1|n(N) = k) &= \frac{P(V_{N+1} = 1, n(N) = k)}{P(n(N) = k)} \\ &= \frac{\int_0^1 P(n(N) = k|p) f(p) p \cdot dp}{\int_0^1 P(n(N) = k|p) f(p) \cdot dp} \\ &= \frac{k+1}{N+2} \end{aligned} \quad (5)$$

On the whole, Equation 5 shows how to compute trust values for network devices (or called nodes) in healthcare SDNs. A key is to observe the total number of packets  $N$  and know how many packets, say  $k$ , are benign. The centralized server can thus establish a map of trust among nodes, and detect a potential untruthful device if given a proper threshold. Based on the particular security requirements and settings, security administrators can adjust the threshold accordingly.

### C. Detection Threshold

The studies in [18], [19] showed that recent traffic status would be more important than some very old experiences, in the sense of improving detection accuracy and identification speed. This observation is also echoed in our previous study [32]. To meet this requirement, similar to [18], we adopt a forgetting factor  $\lambda$ , which can allocate less weight to older statistics (i.e., reducing the impact of old events gradually). As a result, if given a time period  $t$ , a node's trust value based on network packets ( $t_{value}^p$ ) can be calculated as below.

$$t_{value}^p = \lambda \frac{k_t^p + 1}{N_t^p + 2} \quad (6)$$

As healthcare environments are more sensitive than traditional networks, some additional signatures, called self-defined rules, can be developed to identify some sensitive keywords by security administrators [32]. In this environment, a low false rate is highly required as any falsely blocked devices can result in an unexpected accident. For such a trust-based IDS scheme, a dynamic blacklist can be employed to block malicious devices. Then, SDN controller can configure data flow to bypass those malicious locations.

The detailed process of generating a blacklist can be tuned accordingly in terms of IDS signatures and self-defined signatures.

- If a packet matches an IDS signature, then the node will be blacklisted instantly.
- If a packet only matches a self-defined signature, then the node will not be blacklisted at once, but depends on its trust value and relevant threshold.

**Device profile.** Malicious traffic is often accompanied by abnormal behavior. Our survey participants expressed the need for any security solution to consider the device profile, as healthcare organizations usually have strict policies on the use of medical devices. In some countries, medical devices and their usage are (legally) regulated. Hence, unusual usage can be considered as abnormal behavior. In this case, it is not hard to identify unusual devices if any security policy is given, i.e., a whitelist to define what is good to the network. Similarly, we can apply Bayesian inference for evaluating the trustworthiness of devices based on their profile. For a given period  $t$ , a device's trust value ( $t_{value}^d$ ) can be computed as below.

$$t_{value}^d = \lambda \frac{k_t^d + 1}{N_t^d + 2} \quad (7)$$

In Equation 7,  $k_t^d$  denotes the normal profile and  $N_t^d$  denotes the total number of profile. In this work, we focus on *visited websites* and *email address*, two key attributes highlighted by the surveyed participants.

To facilitate trust evaluation, we develop the following single metric,  $t_{value}^{total}$ :

$$t_{value}^{total} = W_1 \times t_{value}^p + W_2 \times t_{value}^d \quad (8)$$

In Equation 8,  $W_1$  and  $W_2$  are weight values and  $W_1 + W_2 = 1$ . Therefore, a device can be blacklisted as malicious if the trust values decrease below a threshold of  $T \in [0, 1]$ . As the blacklist is dynamic, it has to check  $t_{value}$  periodically.

- If  $t_{value} \geq T$ , then the device in the blacklist should be deleted.
- If  $t_{value} < T$ , then the device in the blacklist should be maintained.

It is worth emphasizing that a device can be put in the blacklist at once, if it sends only one malicious packet. However, this strategy may cause a high false positive and degrade the performance of medical systems in a practical

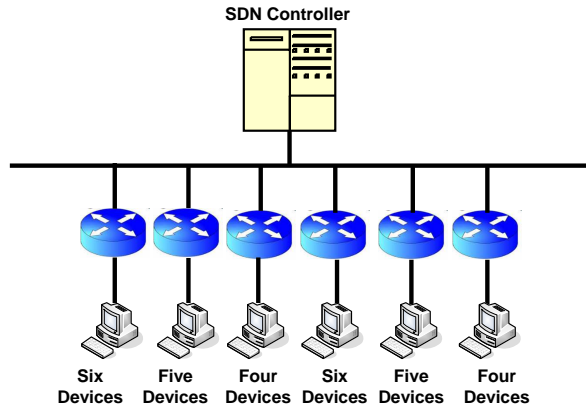


Fig. 4. High-level framework for the simulated SDN environment.

healthcare network. This is the main reason why our approach is dynamic, providing much flexibility of recovering false detected devices. In practice, this mechanism can evaluate the trustworthiness of a device based on its long-time behavior and provide more flexibility for IT administrators to control and manage the network in the SDN controller.

## V. EVALUATION

In this section, we collaborate with practical organizations in healthcare domains and evaluate the performance of our mechanism in both simulated and real healthcare SDN environments.

### A. Methodology and Experimental Results

In the evaluation, we mainly conduct two experiments to investigate the performance of our approach as follows.

- In the first evaluation, we evaluate our trust-based approach in a simulated healthcare SDN environment under both honest and dishonest environments. (see Section V-A1)
- In the second evaluation, we evaluate our trust-based approach in a healthcare SDN environment, in collaboration with a healthcare organization located in China (i.e., one of the 12 surveyed organizations). (see Section V-A2)

**1) Simulated Environment Evaluation:** In this evaluation, we simulated a SDN environment in our lab to explore the feasibility of our approach. In particular, we used OpenDay-Light (ODL)<sup>1</sup> as the SDN controller (on a server with an Intel(R) Core (TM)2, Quad CPU 2.66GHz), and Open vSwitch (OVS)<sup>2</sup> as SDN-enabled switches. We used the open source Snort to detect malicious traffic. In other words, the simulated environment consists of one SDN controller and six SDN switches. Up to 30 devices were randomly connected to these switches. Figure 4 depicts the high-level framework for the simulated SDN environment.

To simulate a healthcare environment, we applied 70 self-defined rules (suggested by our survey participants) in addition to Snort signatures for traffic inspection, and developed

<sup>1</sup><https://www.opendaylight.org/>.

<sup>2</sup><http://openvswitch.org/>.

TABLE III  
THE SIMULATION SETTINGS IN OUR EVALUATION.

Parameters	Value	Description
$\lambda$	0.9	forgetting factor
$T_{initial}$	0.5	initial trust value
$(W_1, W_2)$	(0.6, 0.4)	weight values

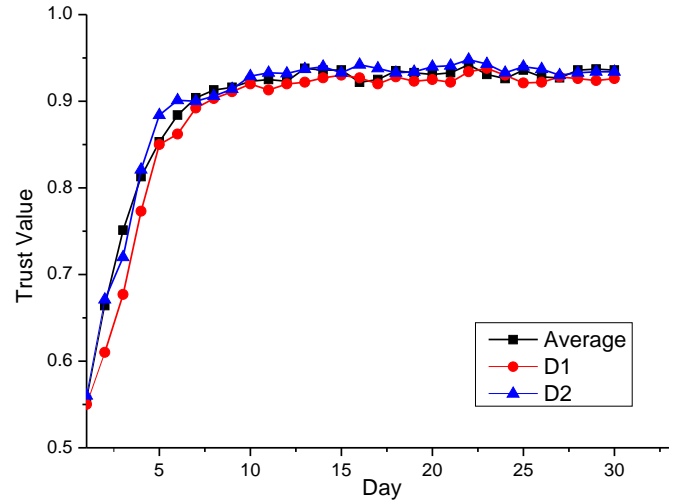


Fig. 5. Trust values of devices under normal environment.

a whitelist for website browsing and email usage. In this work, we compared our approach with the challenge-based intrusion detection mechanism, which focuses on evaluating the trustworthiness of an IDS node through sending challenges [18], [19]. To facilitate the comparison with challenge-based intrusion detection, we set  $\lambda = 0.9$  and initial trust value  $T_{initial} = 0.5$  (details are available on [18], [19]). The simulation parameters are described in Table III. As packet inspection is more intuitive and sensitive,  $t_{value}^p$  has a slightly higher weight ( $W_1 = 0.6$ ).

**Normal scenario.** The average trust value of all devices after launching the network are shown in Fig 5. It is observed that the average trust value becomes stable after some time, under the normal traffic environment. This is because the controller has to gather data from each switch in the network and build a trust matrix. Fig. 5 also shows the trust values of two devices, which converged similar to each other. Based on the trend of trust values, we could select the threshold to 0.9.

**Adversarial scenario.** We randomly selected two highly trusted devices to conduct a betrayal attack with malicious actions, as follows:

- MD-1. This device was configured to send malicious packets, which can trigger IDS alarms.
- MD-2. This device was configured to both generate malicious traffic and act abnormally, e.g., visiting malicious website.

To the best of our knowledge, there has been little work investigating trust management in SDN environments. To make a comparison, we adopted two trust management approaches as a baseline, which are most relevant to this work. The first model was proposed by Duma *et al.* [8]. They developed a P2P-based overlay IDS, which attempted to figure out a



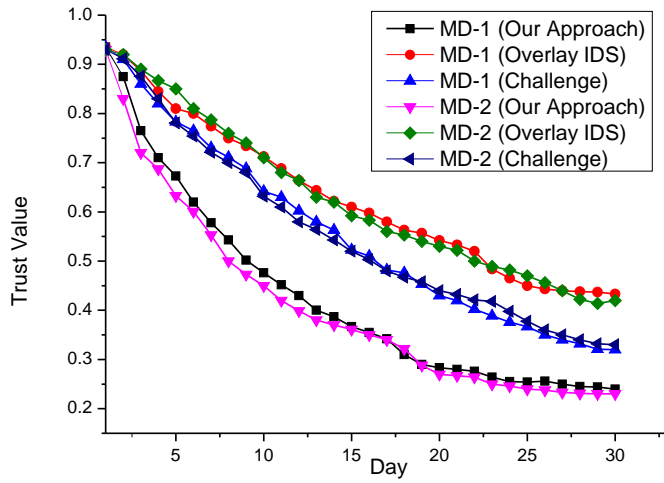


Fig. 6. Trust values of malicious devices of MD-1 and MD-2.

malicious nodes by means of both a trust engine and an adaptive approach for trust management in a distributed IDS network. The second model was proposed by Fung *et al.* [18], [19]. They designed a challenge-based trust management model for identifying malicious nodes in a collaborative IDS network. In the evaluation, we tuned these models to fit a SDN environment and a centralized server were deployed to gather data and compute the trustworthiness of devices.

Fig. 6 depicts the trust values of malicious nodes within the network environment, and we have the following major observations.

- The figure indicates that the challenge-based model could reduce the trust values of malicious nodes faster than the overlay IDS model. This observation is in line with the results in [18], because challenge-based model employs forgetting factor that gives more weight to recent experience.
- For both malicious devices, our approach can decrease their trust values more quickly than the other two trust models. This is because our Bayesian model relies mainly on the evaluation of packet's status for a period of time, which can be more sensitive to traffic dynamics in practice.
- The trust value of MD-2 decreases slightly faster than that of MD-1 computed by our approach, since MD-2 could both generate malicious traffic and perform abnormally. This indicates that profile information has a positive impact on identifying malicious devices. However, its trust value was not greatly affected by the other two models, as they were unable to handle abnormal device profile.

Overall, these results indicate that our approach is viable.

**2) Real-World Evaluation:** In this evaluation, we sought to investigate the performance of our approach in a realistic environment. We collaborated with one of the 12 healthcare organizations to implement our approach in their environment. Due to privacy concerns (e.g., local privacy legislation), we worked with the IT personnel from the organization to build a healthcare SDN (to be part of their network) and deploy

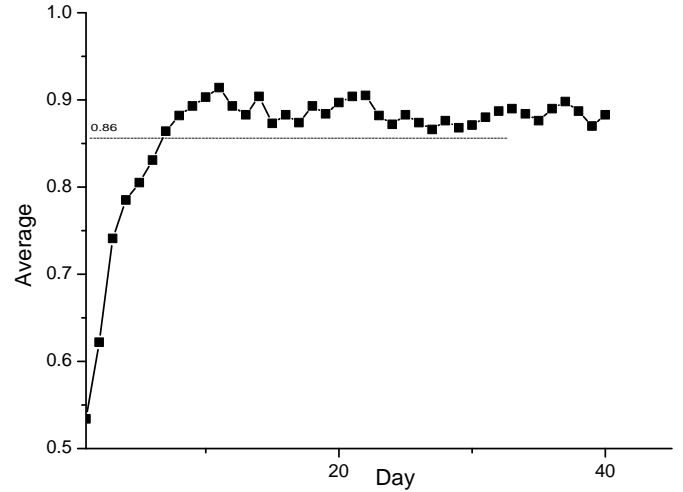


Fig. 7. Trust values of devices under normal traffic in a real-world healthcare SDN.

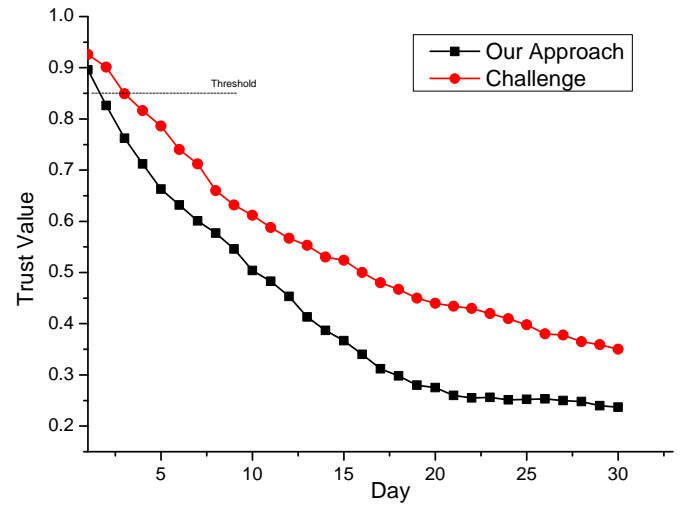


Fig. 8. Trust value of malicious device in a real-world healthcare SDN.

our mechanism in this environment. The healthcare SDN comprises one SDN controller, eight SDN switches and 20 devices (including personal computers and mobile devices). The center had a whitelist for normal websites and email address, and defined up to 245 self-defined rules based on the previous traffic data, including a number of sensitive keywords and unwanted IP addresses. The other settings are similar to Section V-A1.

To determine an appropriate threshold, we run the network for a period of time. The average trust value is depicted in Fig. 7. As compared with the simulation result in Fig. 5, it is found that the trust value in a real environment is more dynamic, due to the complexity of real traffic. This is not surprising. Generally, the average value ranged from 0.86 to 0.92. In this case, we selected 0.85 as the detection threshold.

**Adversarial scenario.** Similar to Section V-A1, we randomly selected two devices to conduct malicious actions including generating of malicious packets and acting abnormally. Fig. 8 presents the average trust value of malicious devices under this scenario. The observation is similar to Section V-A1. That is, our Bayesian approach has the capability of reducing the trust

TABLE IV  
CPU WORKLOAD OF CONTROLLER AND SWITCHES UNDER DIFFERENT SCENARIOS.

Controller Side Condition	Average CPU (%)	Max CPU (%)
Normal scenario	15.3	26.7
Adversary scenario	33.7	41.3
Switch Side Condition	Average CPU (%)	Max CPU (%)
Normal scenario	6.8	13.7
Adversary scenario	18.4	30.3

value of malicious device more quickly than the challenge-based approach. The experimental results demonstrated that our approach is effective in identifying malicious devices in a healthcare SDN environment.

### B. Workload

Intuitively, deploying additional security mechanisms may result in higher CPU load due to communication and operations. In this part, we evaluate the additional workload due to our approach for the main IDS controller (SDN controller side) and IDS agents (switch side).

On the switch side, many operations can increase the workload such as collecting packet and device profile information, communicating with the controller and so on. On the controller side, the workload can be caused by gathering statistical information from switches, calculating trust values, updating flow tables and enforcing security policies.

Table IV presents the CPU workload on both controller and switch sides under normal and adversary scenarios in the real-world healthcare SDN environment. The main observations are described as below.

- The CPU load on controller side is heavier than that on switch side. For example, the CPU load is 15.3% and 6.8% for the controller and switch under normal scenario, respectively. This is because the controller has to collect information and manage the entire network.
- Generally, the CPU load on both sides would become significantly heavier in a hostile scenario, as compared to the normal traffic scenario. For instance, the CPU increased 33.7% on average under attack as compared to 15.3% under normal traffic. This is because more packets would be exchanged and transmitted under the abnormal traffic scenario (i.e., resulting in an increase of malicious packets), in addition to the communication increased between main IDS and IDS agents.

### C. Scalability Investigation

In order to validate the performance and explore the scalability of our Bayesian approach in different scenarios (i.e., with more devices), we further collaborated with the same healthcare organization and evaluated our proposed mechanism using 50 devices (with 15 switches) and 70 devices (with 20 switches), respectively. Moreover, we collaborated with another of the healthcare organizations in China, which has a similar infrastructure with the first healthcare organization, to

build a healthcare SDN with 100 devices (with 31 switches). This (second) healthcare organization maintained a whitelist for normal websites and email address, and had 260 self-defined rules in relation to sensitive keywords and unwanted IP addresses.

Fig. 9 shows the average trust values of devices under these scenarios. It is visible that the average trust values of devices could gradually converge and ranged from 0.85 to 0.93 regarding different conditions. This observation is similar to our previous evaluations; hence, we chose 0.85 to be the detection threshold.

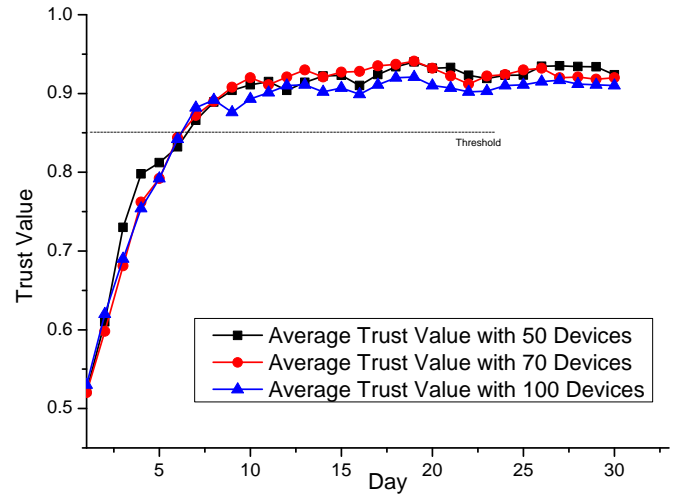


Fig. 9. Trust values of devices under various normal scenarios.

To validate the performance of our approach against malicious nodes, we randomly selected a ratio of 1/5, 1/4 and 1/3 highly trusted devices to conduct a betrayal attack (i.e., behaved maliciously suddenly), respectively. Taking the scenario with 50 devices as an example, there could be 10, 13 and 17 malicious devices accordingly. Fig. 10 depicts the average trust values of malicious devices under different adversarial scenarios. The trust values of malicious devices were observed to decrease rapidly across different scenarios. Moreover, a faster decrease of average trust values could be caused by an increase of malicious devices. For instance, under the scenario with 50 devices, the average trust value of 17 malicious devices could decrease a bit faster than that of 13 malicious devices.

As a comparison, Fig. 11 compares the trust value of malicious devices between our approach and the challenge-based trust mechanism. It is found that the trust value under our approach decreased much faster than those under the challenge-based approach. This is because our approach is more sensitive to traffic changes. Fig. 12 then shows the average trust values of malicious devices with the challenge-based approach under different adversarial scenarios. Overall, these results are in line with the observations in the other evaluations reported above, demonstrating that our Bayesian approach can work well in detecting malicious devices in a fast manner and can provide good scalability in distinct scenarios.

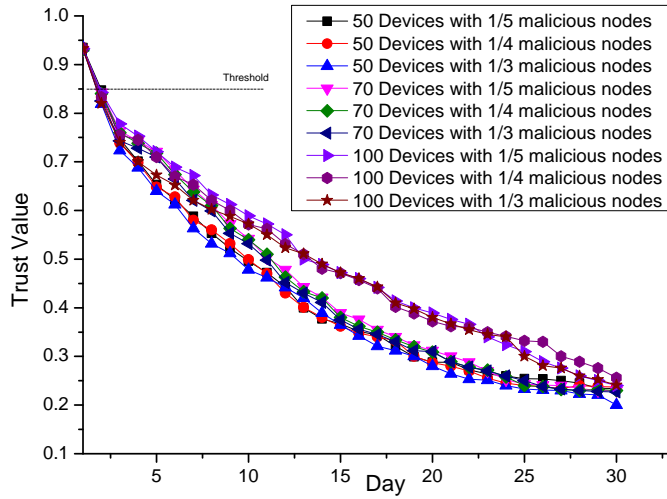


Fig. 10. Trust values of malicious devices with our approach under various adversarial scenarios.

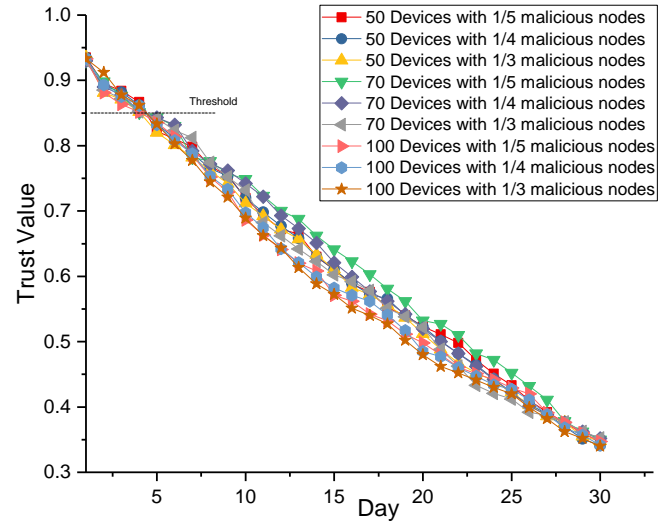


Fig. 12. Trust values of devices with challenge-based approach under various adversarial scenarios.

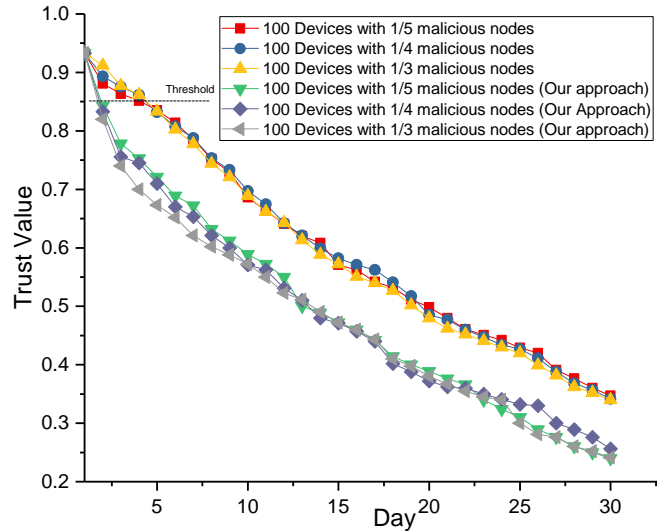


Fig. 11. A comparison of trust values under the adversarial scenario.

## VI. DISCUSSION AND CHALLENGES

Based on the findings of our survey and the evaluations reported in the preceding sections, we will now discuss several limitations and open challenges in securing medical networks.

*a) Threshold:* In comparison to the threshold in a wired network (e.g., 0.75 [27]) or a wireless sensor network (e.g., 0.72 [28]), healthcare networks have a higher threshold. This indicates that healthcare traffic is not as complex as a conventional network, because there are only less connected devices than a convention wired network. On the other hand, healthcare network would implement a more strict detection rules. Therefore, in practice, it could be easier to develop compact and effective security schemes to save energy and storage in some resource-limited medical devices.

*b) Behavioral profile:* In this work, we only employed two most common profile features for device profile based on the findings from our survey. In practice, more features will need to be considered in order to establish a more precise

profile. However, there is also a need to develop a robust security scheme with few features, as a medical network is extremely sensitive where not all expected features are available in some cases. This is an open challenge in this area.

*c) Large traffic volume:* With the advent of big data, traffic volume will significant increase in medical networks, particularly in the near future as more medical devices are Internet-connected. The data could be difficult to be managed efficiently by on-hand techniques, tools and devices. To mitigate this issue, traffic sampling is a potential solution for deploying IDSs in a large-sized network [14]. In addition, pre-filtration can be considered to reduce unwanted traffic and lighten the processing burden [27], [30].

*d) IT experts in the healthcare area:* It is not surprised that manufactures handle and maintain the medical devices and their security in a traditional way. However, more medical devices are becoming Internet-enabled due to the coming era of Internet of things (IoT), demanding many IT experts in setting those medical devices more frequently, i.e., configuring embedded systems, examining network traffic and potential security breaches. The lack of IT experts, especially security experts, in healthcare organizations exposes a big hole for the security in healthcare domain.

*e) Security policy enforcement:* Due to the sensitivity of healthcare networks, there is a great need to apply and enforce security policies in different network levels, i.e., deploying access control policy to ensure medical device to be accessed by only trusted users. This reiterates the need for more cyber security experts in protecting healthcare environments. Further, security policies would not be fixed but have to be reconfigured based on a specific environment. That is, distinct security policies should be applied in different organizations. Having in place standards to guide the development of security policies is another key consideration.

*f) Implementation of additional security mechanisms:* Fig. 10 showed that the curves of 100 devices were higher than the ones for 50 or 70 nodes, though the curves reached the same point in the end. These may be caused by communication

delay or other factors. This is an interesting topic that can be investigated and validated in our future work. For example, some additional security mechanisms can be implemented to narrow the curve gap.

## VII. CONCLUSION

As healthcare organizations become more connected and digitized (e.g., digitization of patient records, prescription ordering, communication between doctors and patients), ensuring the security of Internet-enabled devices and the system without compromising performance and usability will also become increasingly challenging. Software-defined networking (SDN) allows the decoupling of network control from the data plane, but SDN based solutions are not generally designed to mitigate against insider threats.

In this paper, we surveyed stakeholders from 12 healthcare organizations in Hong Kong, Singapore and China to obtain in-depth understanding of the system design requirements in medical networks. Motivated by our findings, we focus on the identification of insider attacks in healthcare SDNs by proposing a trust-based Bayesian approach for such environment. Findings from our evaluations in both simulated and real-world environments (in collaboration with two of the 12 healthcare organizations) demonstrated that the effectiveness and scalability of our approach in detecting malicious devices under various conditions. Future work could include investigating how to further improve the detection sensitivity and validating the performance of our approach in an even larger environment.

## ACKNOWLEDGMENT

We would like to thank all surveyed healthcare managers and IT administrators from the relevant hospitals and clinics in Hong Kong, China and Singapore for their great support and helpful suggestions regarding our mechanism design and implementation.

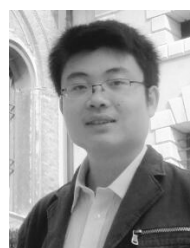
## REFERENCES

- [1] A. AlEroud and I. Alsmadi. Identifying cyber-attacks on software defined networks: An inference-based intrusion detection approach. *Journal of Network and Computer Applications* vol. 80, pp. 152-164, 2017.
- [2] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho. Trust-Based Intrusion Detection in Wireless Sensor Networks. In *Proceedings of the 2011 IEEE International Conference on Communications (ICC)*, pp. 1-6, 2011.
- [3] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection. *IEEE Transactions on Network and Service Management* 9(2), 169-183, 2012.
- [4] C. Beek, C. McFarland, and R. Samani. McAfee Report: Health Warning-Cyberattacks are targeting the health care industry. (October 2016) Available at: <https://www.mcafee.com/us/resources/reports/rp-health-warning.pdf>.
- [5] B. Chappell, and M. Penman. Ransomware Attacks Ravage Computer Networks In Dozens Of Countries. <http://www.npr.org/sections/thetwo-way/2017/05/12/528119808/large-cyber-attack-hits-englands-nhs-hospital-system-ransoms-demanded>
- [6] H. Chen, H. Wu, J. Hu, and C. Gao. Event-based Trust Framework Model in Wireless Sensor Networks. In *Proceedings of the 2008 International Conference on Networking, Architecture, and Storage (NAS)*, pp. 359-364, 2008.
- [7] J.-H. Cho, A. Swami, and I.-R. Chen. A Survey on Trust Management for Mobile Ad Hoc Networks. *IEEE Communications Surveys & Tutorials* 13(4), 562-583, 2011.
- [8] C. Duma, M. Karresand, N. Shahmehri, and G. Caronni, "A Trust-Aware, P2P-Based Overlay for Intrusion Detection," In: *Proceedings of the 17th International Workshop on Database and Expert Systems Applications (DEXA)*, pp. 692-697, 2006.
- [9] J.M. Gonzalez, M. Anwar, and J.B.D. Joshi. A Trust-based Approach against IP-Spoofing Attacks. In *Proceedings of the 9th International Conference on Privacy, Security and Trust (PST)*, pp. 63-70, 2011.
- [10] A.K. Ghosh, J. Wanken, and F. Charron. Detecting Anomalous and Unknown Intrusions Against Programs. In *Proceedings of the 1998 Annual Computer Security Applications Conference (ACSAC)*, pp. 259-267, 1998.
- [11] P.C. Evans and M. Annunziata. Industrial Internet, Pushing the Boundary of Mind and Machines. (November, 2012) Available at: [http://www.ge.com/sites/default/files/Industrial\\_Internet.pdf](http://www.ge.com/sites/default/files/Industrial_Internet.pdf).
- [12] G. Grispos, W. B. Glisson, and K.-K. R., Choo. Medical Cyber-Physical Systems Development: A Forensics-Driven Approach. In *Proceedings of IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE 2017)*, pp. 108-114, 2017.
- [13] J. Guo, A. Marshall, and B. Zhou. A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for Mobile Ad Hoc Networks. In *Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 142-149, 2011.
- [14] T. Ha, S. Kim, N. An, J. Naranitaya, C. Jeong, J. Kim, and H. Lim. Suspicious traffic sampling for intrusion detection in software-defined networks. *Computer Networks* vol. 109, pp. 172-182, 2016.
- [15] P. Harries. The Prognosis for Healthcare Payers and Providers: Rising Cybersecurity Risks and Costs. (December, 2014) Available at: <http://usblogs.pwc.com/cybersecurity/the-prognosis-for-healthcare-payers-and-providers-rising-cybersecurity-risks-and-costs/>.
- [16] R. Hasan, S. Zawood, S. Noor, M.M. Haque, and D. Burke. How Secure is the Healthcare Network from Insider Attacks? An Audit Guideline for Vulnerability Analysis. In: *Proceedings of the 40th Annual Computer Software and Applications Conference*, pp. 417-422 (2016)
- [17] J. Healey, N. Pollard, and B. Woods. The Healthcare Internet of Things: Rewards and Risks. (March 2015) Available at: <http://www.mcafee.com/mx/resources/reports/rp-healthcare-iot-rewards-risks.pdf>.
- [18] C.J. Fung, O. Baysal, J. Zhang, I. Aib, and R. Boutaba. Trust Management for Host-Based Collaborative Intrusion Detection. In: *Proceedings of the 19th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM)*, pp. 109-122, 2008.
- [19] C.J. Fung, O. Baysal, J. Zhang, I. Aib, and R. Boutaba. Robust and scalable trust management for collaborative intrusion detection. In: *Proceedings of the 2009 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 33-40, 2009.
- [20] S. Larson. Why hospitals are so vulnerable to ransomware attacks. <http://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html>
- [21] Z. Li, Y. Chen, and A. Beach, "Towards Scalable and Robust Distributed Intrusion Alert Fusion with Good Load Balancing," In: *Proceedings of the 2006 SIGCOMM workshop on Largescale attack defense (LISA)*, pp. 115-122, 2006.
- [22] W. Li, Y. Meng, and L.F. Kwok. Enhancing Trust Evaluation Using Intrusion Sensitivity in Collaborative Intrusion Detection Networks: Feasibility and Challenges. In *Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS)*, pp. 518-522, 2013.
- [23] W. Li, W. Meng, and L.F. Kwok. Design of Intrusion Sensitivity-Based Trust Management Model for Collaborative Intrusion Detection Networks. In *Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIPTM)*, pp. 61-76, 2014.
- [24] W. Li, W. Meng, and L.F. Kwok. A Survey on OpenFlow-based Software Defined Networks: Security Challenges and Countermeasures. *Journal of Network and Computer Applications*, vol. 68, pp. 126-139, 2016
- [25] W. Li, W. Meng, L.F. Kwok, and H.H.S. Ip. Enhancing Collaborative Intrusion Detection Networks Against Insider Attacks Using Supervised Intrusion Sensitivity-Based Trust Management Model. *Journal of Network and Computer Applications* vol. 77, pp. 135-145, 2017.
- [26] Y. Meng and L.-F. Kwok. Enhancing False Alarm Reduction Using Voted Ensemble Selection in Intrusion Detection. *International Journal of Computational Intelligence Systems* 6(4), pp. 626-638, 2013.
- [27] Y. Meng, L.F. Kwok, and W. Li. Towards Designing Packet Filter with A Trust-based Approach using Bayesian Inference in Network Intrusion Detection. In *Proceedings of the 8th International Conference*

- on Security and Privacy in Communication Networks (SECURECOMM), pp. 203-221, 2012.
- [28] Y. Meng, W. Li., and L.-F. Kwok. Evaluation of Detecting Malicious Nodes Using Bayesian Model in Wireless Intrusion Detection. In *Proceedings of The 7th International Conference on Network and System Security (NSS)*, pp. 40-53, 2013.
- [29] W. Meng, W. Li., and L.-F. Kwok. EFM: Enhancing the Performance of Signature-based Network Intrusion Detection Systems Using Enhanced Filter Mechanism. *Computers & Security* vol. 43, pp. 189-204, 2014.
- [30] W. Meng and L.-F. Kwok. Adaptive Blacklist-based Packet Filter with A Statistic-based Approach in Network Intrusion Detection. *Journal of Network and Computer Applications* vol. 39, pp. 83-92, 2014.
- [31] W. Meng, W. Li, and L.-F. Kwok. Design of Intelligent KNN-based Alarm Filter Using Knowledge-based Alert Verification in Intrusion Detection. *Security and Communication Networks* 8(18), pp. 3883-3895, 2015.
- [32] W. Meng, W. Li, Y. Xiang, and K.K.R. Choo. A Bayesian Inference-based Detection Mechanism to Defend Medical Smartphone Networks Against Insider Attacks. *Journal of Network and Computer Applications*, vol. 78, pp. 162-169, 2017.
- [33] ONFA Healthy Dose of SDN. (August 2016) Available at: [https://www.opennetworking.org/?p=2411&option=com\\_wordpress&Itemid=316](https://www.opennetworking.org/?p=2411&option=com_wordpress&Itemid=316).
- [34] J. Peng, K.-K. R. Choo, and H. Ashman. User profiling in intrusion detection: A review. *Journal of Network and Computer Applications*, vol. 72, pp. 14-27, 2016.
- [35] P.A. Porras and R.A. Kemmerer. Penetration State Transition Analysis: A Rule-based Intrusion Detection Approach. In *Proceedings of the 8th Annual Computer Security Applications Conference (ACSAC)*, pp. 220-229, 1992.
- [36] M.J. Probst and S.K. Kasera. Statistical Trust Establishment in Wireless Sensor Networks. In *Proceedings of the 2007 International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 1-8, 2007.
- [37] F. Wang, C. Huang, J. Zhang, and C. Rong. IDMTM: A Novel Intrusion Detection Mechanism based on Trust Model for Ad-Hoc Networks. In *Proceedings of the 22nd IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pp. 978-984, 2008.
- [38] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication, pp. 800-894, 2007. <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>
- [39] R.A. Shaikh, H. Jameel, B.J. d'Auriol, H. Lee, S. Lee, and Y.J. Song. Group-based Trust Management Scheme for Clustered Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems* 20(11), 1698-1712, 2009.
- [40] Snort: An open source network intrusion prevention and detection system (IDS/IPS). Homepage: <http://www.snort.org/>
- [41] Symantec. Networked Medical Devices: Security and Privacy Threats. (June 2015) Available at: [https://www.symantec.com/content/en/us/enterprise/white\\_papers/b-networked\\_medical\\_devices\\_WP\\_21177186\\_en-us.pdf](https://www.symantec.com/content/en/us/enterprise/white_papers/b-networked_medical_devices_WP_21177186_en-us.pdf).
- [42] Y.L. Sun, W. Yu, Z. Han, and K. Liu. Information Theoretic Framework of Trust Modelling and Evaluation for Ad Hoc Networks. *IEEE Journal of Selected Areas in Communications*, vol. 24, no. 2, pp. 305-317, 2006.
- [43] E. Tara. 92% of Healthcare IT Admins Fear Insider Threats. (April 2015) Available at: <https://www.infosecurity-magazine.com/news/92-of-healthcare-it-admins-fear/>.
- [44] T.A. Tuan, "A Game-Theoretic Analysis of Trust Management in P2P Systems," In: *Proceedings of the 1st International Conference on Communications and Electronics (ICCE)*, pp. 130-134, 2006.
- [45] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and Survey of Collaborative Intrusion Detection," *ACM Computing Surveys*, vol. 47, no. 4, 2015.
- [46] Wireshark: Network Protocol Analyzer. Homepage: <http://www.wireshark.org/>
- [47] P.A.H. Williams and A.J. Woodward. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices: Evidence and Research* 8, 305-316, 2015.
- [48] Y.-S. Wu, B. Foo, Y. Mei, and S. Bagchi, "Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS," In: *Proceedings of the 2003 Annual Computer Security Applications Conference (ACSAC)*, pp. 234-244, 2003.
- [49] T. Zahariadis, P. Trakadas, H.C. Leligou, S. Maniatis, and P. Karkazis. A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks. *Wireless Personal Communications* 69(2), 1-22, 2012.
- [50] J. Zhang, R. Shankaran, M.A. Orgun, V. Varadharajan, and A. Sattar. A Dynamic Trust Establishment and Management Framework for Wireless Sensor Networks. In *Proceedings of the 2010 IEEE/IFIP International*

*Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 484-491, 2010.

- [51] C.V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection," *Computers & Security*, vol. 29, no. 1, pp. 124-140, 2010.



**Weizhi Meng** is currently an assistant professor in the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. He received his B.Eng. degree in Computer Science from the Nanjing University of Posts and Telecommunications, China and obtained his Ph.D. degree in Computer Science from the City University of Hong Kong (CityU), Hong Kong in 2013. He was known as Yuxin Meng and prior to joining DTU, he worked as a research scientist in Infocomm Security (ICS) Department, Institute for Infocomm Research, Singapore, and as a senior research associate in CityU after graduation. He won the Outstanding Academic Performance Award during his doctoral study, and is a recipient of The HKIE Outstanding Paper Award for Young Engineers/Researchers in 2014 and a co-recipient of the Best Student Paper Award from the 10th International Conference on Network and System Security (NSS) in 2016. His primary research interests are cyber security and intelligent technology in security including intrusion detection, mobile security and authentication, HCI security, cloud security, trust computation, web security, malware and vulnerability analysis. He also shows a strong interest in applied cryptography. He is a member of IEEE.



**Kim-Kwang Raymond Choo** received the Ph.D. in Information Security from Queensland University of Technology, Australia. He currently holds the cloud technology endowed professorship at the University of Texas at San Antonio, and is an associate professor at University of South Australia. He was named one of 10 Emerging Leaders in the Innovation category of The Weekend Australian Magazine / Microsoft's Next 100 series in 2009, and is the recipient of various awards including ESORICS 2015 Best Research Paper Award, Highly Commended Award from Australia New Zealand Policing Advisory Agency, British Computer Society's Wilkes Award, Fulbright Scholarship, and 2008 Australia Day Achievement Medallion. He is a Fellow of the Australian Computer Society, and a Senior Member of IEEE.



**Steven Furnell** is a professor of information security and leads the Centre for Security, Communications & Network Research at Plymouth University. He is also an Adjunct Professor with Edith Cowan University in Western Australia and an Honorary Professor with Nelson Mandela Metropolitan University in South Africa. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 280 papers in refereed international journals and conference proceedings, as well as books including *Cybercrime: Vandalizing the Information Society* and *Computer Insecurity: Risking the System*. Prof. Furnell is the current Chair of Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a member of related working groups on security management, security education, and human aspects of security. He is also a board member of the Institute of Information Security Professionals, and chairs the academic partnership committee and southwest branch.





**Athanasios V. Vasilakos** is recently Professor with the Lulea University of Technology, Sweden. He served or is serving as an Editor for many technical journals, such as the IEEE Transactions on Network and Service Management, IEEE Transactions on Cloud Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cybernetics, IEEE Transactions on Nanobioscience, IEEE Transactions on Information Technology in Biomedicine, ACM Transactions on Autonomous and Adaptive Systems, and the IEEE Journal on

Selected Areas in Communications.



**Christian W. Probst** is Professor for Cyber Security at the Unitec Institute of Technology in Auckland, New Zealand, and Director of the High Technology Transdisciplinary Research Network. His research interests are in the area of cyber security, organisational security, and programming languages, and his work ranges from organisational security and detection and mitigation of insider threats and social engineering, over cloud infrastructures, virtual machines, and programming languages, to power-aware computing systems and runtime systems for

embedded systems. In his research, Christian combines modelling and analysis of systems to develop systems with guaranteed properties, or to assess these properties. His research leads to practical solutions as part of tools or processes that can be applied to any kind of systems, but especially to the security of networked computer systems and organisations, and to runtime systems including processors and virtual machines. He has an MSc and a PhD from Saarland University, Germany. Before joining Unitec in 2018, he has worked at the Technical University of Denmark and University of California, Irvine, USA.